M2M HROZBY

Válka strojů

M2M je zkratka pro machine-to-machine (stroj-stroj) neboli technologii podporující drátovou či bezdrátovou komunikaci mezi stroji.

Příkladem technologie M2M může být například soustava zařízení monitorujících provoz ve městě. Ta dále předávají informace dopravním semaforům a přispívají tak k regulaci toku dopravy. Technologie M2M se využívá v telemetrii, při sběru dat, pro vzdálené ovládání, v robotice, pro vzdálený monitoring, pro sledování stavu různých zařízení, pro kontrolu silniční dopravy, pro vzdálenou diagnostiku i údržbu, v bezpečnostních systémech, v logistických službách nebo v telemedicíně.

Pouze móda?

Ačkoli v současné době může komunikace typu stroj-stroj působit spíše jako „módní záležitost", která se reálně využívá jen minimálně, je potenciál „internetu věcí" vpravdě nedozírný. S pokroky v oblasti malých levných počítačů, s šířením chytrých zařízení, rozvojem broadbandu (širokopásmového připojení) a lepšími vlastnostmi bezdrátových sítí je pouze otázkou času, kdy se takzvaná hyperkonektivita – kde mezi sebou stroje komunikují navzájem, bez lidských zásahů – stane součástí každodenního života. Stačí se však podívat, jaká bezpečnostní rizika doprovázejí nástup v podstatě každé nové technologické vlny, aby vám bylo jasné, že i s rozvojem M2M přichází stále rostoucí počet čím dál tím rozmanitějších hrozeb ze strany potenciálních útočníků.

Potenciál ke zneužití

Popularita operačního systému Windows jej činí obzvláště lákavým k různým útokům. Skutečnost, že se Windows XP ve stále větší míře implementují do bankomatů, zábavních systémů v letadlech, a dokonce do příští generace vybavení britského vojenského námořnictva, by měla donutit k zamyšlení snad každého, kdo se zabývá bezpečností. Tam, kde jsou bankomaty propojené se systémy v backoffice, může dojít maximálně ke „ztrátě transakce". Ale jak dlouho může trvat, než budou i zábavní systémy v letadlech propojeny s leteckými „backend systémy" a učiní tak z pouhého restartu mnohem závažnější záležitost? A co implementace Windows do příští generace útočných ponorek, kde bude OS od Microsoftu ovládat a spravovat kritické obranné systémy? Tehdy se zranitelnosti mohou stát opravdu smrtelnými!

Nové cíle útoků

Kromě vysokého stupně využívání této standardizované technologie (myšleno Windows) začínají se objevovat i další cíle potenciálních útoků. Bezpečnostní výzkumníci prokázali, jak je snadné získat důvěrné informace z kreditních a debetních karet postavených na technologii RFID (potenciál RFID k nastolení nové „business inteligence" je přitom hlavním tahounem M2M trendu). Ve zkušebním testu bylo odhaleno, že mnohé z bezkontaktních platebních karet postrádají jakoukoli formu šifrovací či jiné technologie k ochraně dat. Banky a finanční domy však tvrdí, že tyto problémy mezitím vyřešily a zajistily, aby kartám, které jsou dnes v užívání, nechyběla kvalitní ochrana před útoky. V tom případě je však namístě následující otázka: „Jsou-li implementovaná řešení tak bezpečná, proč se maximální limity u těchto karet stále pohybují na tak nízké úrovni?"

Národní hrozba

V širším měřítku mohou být útoky spouštěny také na národní bázi, což je z poslední doby patrné například na případech v Estonsku. Účtovací systémy a bankomaty lze „shodit", vozidla s integrovanými funkčními systémy lze zastavit – to vše s úmyslem získat pozornost veřejnosti a způsobit hromadný rozvrat. Podíváme-li se na vše z tohoto úhlu pohledu, musí každý uznat, že bezpečnostní ohledy společnosti fungující skrze M2M rozhodně nejsou zanedbatelné.

Snižování rizika

M2M je kritickou záležitostí, jež je zdánlivě na pokraji masové adopce. Dle odhadů bude letos prodáno 10 miliard mikroprocesorů, které se integrují do všeho – od počítačů až po kávovary. Ačkoli je jen malá šance, že se technologická revoluce ve jménu bezpečnosti zpomalí, experti ze společnosti McAfee zastávají názor, že je potřeba dbát na rostoucí rizika a podniknout adekvátní kroky k tomu, aby konzumenti mohli těžit z pokroku za co nejnižšího rizika. S automatizovanou komunikací přichází více možností a vyšší efektivita, zároveň s tím ovšem nastupuje i potenciální nestabilita a odpovídající zodpovědnost. I proto jsou plány firem pro mimořádné případy opravdu kritické.

Zdroj: McAfee

VÝZKUM IBM X-FORCE

Spam útočí přes PDF

V roce 2005 objevili spammeři novou techniku, jak se vyhnout systémům, které detekují nevyžádanou poštu na základě rozpoznávání textu – obrázkový spam. Tato aktivita dominovala na konci roku 2006, kdy obrázkový spam tvořil přibližně třetinu veškerého spamu. V současné době sleduje výzkumný tým IBM X-Force nový trend: využití PDF spamu. Na základě jeho průzkumu tvořil PDF spam 3 – 4 % veškerého spamu zaznamenaného v období od 26. června tohoto roku. V pátek 6. července dosáhl jeho podíl na veškerém spamu 6 – 8 %.

Pokud se bude spam založený na PDF vyvíjet stejným způsobem jako obrázkový spam, musíme se připravit na možnost, že by PDF spam mohl dosáhnout až 20% podílu na veškerém spamu. Více informací naleznete v blogu Ralfa Ifferta, výzkumníka IBM Internet Security Systems, a to na adrese **http://blogs.iss.net/archive/PDF%20Spam.html**.

NOVINKA V ŽEBŘÍČKU MALWARU

„Animovaný trojský kůň" poražen

Podle výsledků statistického systému ESET ThreatSense.Net byl v červenci globálně nejrozšířenější virovou hrozbou opět Win32/TrojanDownloader.Ani.Gen. V Česku se však tato infiltrace umístila až na druhém místě, přeskočil ji trojský kůň Win32/Spy.VBStat.J s rekordním podílem 6,36 % na celkovém počtu infiltrací šířených u nás.

Win32/Spy.VBStat.J je trojský kůň (jehož podstatou je knihovna DLL), který sbírá informace o hardwarovém a programovém vybavení počítače. Škůdce se šíří pomocí jiného malwaru a k jeho šíření napomáhá i variabilní velikost knihovny DLL. V globálním žebříčku byl v červenci na druhém místě červ Win32/Rjump.A, který po napadení umožňuje vzdálený přístup útočníka na infikovaný počítač. V Česku byl na druhém místě již zmíněný exploit Win32/TrojanDownloader.Ani.Gen.

Na třetím místě globálního žebříčku se zachytil INF/Autorun, což jsou různé rodiny červů, kteří vždy podobným způsobem infikují soubory typu autorun.ini (typicky se šíří prostřednictvím USB klíčů), aby zajistili své spuštění a následné napadení počítače. U nás byl na třetím místě trojský kůň Win32/BHO.G, který se na napadeném počítači nainstaluje jako Browser Helper Object v prohlížeči Internet Explorer a monitoruje vše, co uživatel přes tento prohlížeč udělá. Získává tak seznam navštívených webových stránek a hesla zadávaná při přihlašování k e-mailu nebo k internetovému bankovnictví.

Top 10 infiltrací: červenec 2007 – Česká republika

Pořadí	Virová hrozba	Podíl na celkovém počtu infiltrací
1.	Win32/Spy.VBStat.J trojan	6,36 %
2.	Win32/TrojanDownloader.Ani.Gen	4,03 %
3.	Win32/BHO.G	3,97 %
4.	Win32/Adware.Virtumonde	3,30 %
5.	Win32/Adware.Virtumonde.FP	1,98 %
6.	Win32/Stration.XW	1,96 %
7. (*)	probably unknown NewHeur_PE virus	1,74 %
8.	Win32/TrojanProxy.Slaper.C	1,72 %
9.	Win32/Stration	1,68 %
10.	Win32/PSW.Sinowal.Gen	1,66 %

* Používá se pro skupinu nově zachycených infiltrací, které ještě nemají označení. Zdroj: ESET ThreatSense.Net

TIPY MCAFEE

Obtěžují vás spamy?

Společnost McAfee zveřejnila tipy, které vám pomohou omezit množství nevyžádané pošty. Několik rad může pomoci ochránit vaši e-mailovou adresu tak, aby se nestala terčem spammerů.

► Na spam nikdy neodpovídejte. Pokud na spam odpovíte (a to včetně žádosti o odstranění ze seznamu adresátů), pouze tím potvrdíte, že vaše e-mailová adresa je platná a že se spam podařilo úspěšně doručit do vaší poštovní schránky. Seznamy funkčních adres jsou pro spammery cennější než adresy neověřené a odesilatelé nevyžádané pošty takové seznamy sami často kupují nebo prodávají.

► Ověřte si, zda je vaše e-mailová adresa pro odesilatele nevyžádané pošty „viditelná". To zjistíte například tak, že zadáte svou adresu do webového vyhledávače. Pokud je adresa nalezena na webových stránkách nebo v diskusních skupinách, pokuste se ji odstranit. Tímto způsobem podstatně snížíte množství nevyžádané pošty.

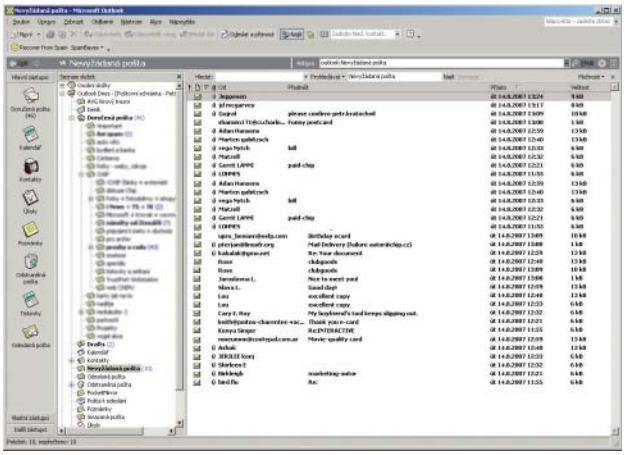
► Zakažte zobrazování obrázků vložených do e-mailových zpráv nebo zprávy s charakterem spamu vůbec neotvírejte. Spam často obsahuje kód, který odesilateli signalizuje, na kolik adres (nebo na jaké konkrétní adresy) se zprávu podařilo doručit a kdo ji otevřel. Většina současných e-mailových programů má z tohoto důvodu ve výchozím nastavení zakázáno zobrazování obrázků vložených do e-mailů.

► Neotevírejte odkazy obsažené v nevyžádané poště, a to ani odkazy sloužící k odhlášení. Tyto odkazy často obsahují kód, který identifikuje e-mailovou adresu příjemce a potvrdí, že spam byl doručen a příjemce na něj reagoval.

► Při vyplňování formulářů na webových stránkách si ověřte zásady, podle nichž se bude nakládat s osobními údaji. Zkontrolujte si, zda tyto údaje nebudou dále prodávány nebo poskytovány třetím stranám. Pro eventuální souhlas s přijímáním e-mailů třetích stran by mělo být k dispozici samostatné políčko pro zaškrtnutí.

► Neodpovídejte na žádné e-maily s žádostí o potvrzení nebo ověření podrobností o svých účtech. Vaše banka nebo společnost vydávající kreditní karty tyto informace již znají a e-mailové potvrzení údajů tohoto typu nevyžadují. Pokud si nejste jisti, zda jsou žádosti o osobní informace od určité společnosti oprávněné, spojte se s ní přímo (například telefonicky) nebo otevřete její stránku ve webovém prohlížeči. Neotevírejte odkazy v e-mailech, protože se může jednat o odkazy podvržené, které směřují na webové servery zneužívané k phishingu.

► Zřiďte si dvě e-mailové adresy, jednu pro osobní komunikaci s přáteli a kolegy a druhou pro účast v elektronických konferencích nebo pro posílání zpráv do diskusních fór nebo na další veřejná místa. Množství obdrženého spamu omezují také složitější/delší e-mailové adresy.



SPAM: **Nástroje proti spamu by měly být až na prvním místě...**

NOVÁ APLIKACE SYMANTECU

Firemní bezpečí z kavárny

Společnost Symantec Corp. představila aplikaci Symantec On-Demand Protection for Outlook Web Access 3.0. Ta by měla nabídnout zákazníkům bezpečné virtuální prostředí pro přístup k poštovním schránkám, kalendářům a souborům aplikace Outlook a také jejich správu prostřednictvím webu.

Podnikoví uživatelé často potřebují k udržení úrovně produktivity přistupovat ke svým e-mailovým účtům z počítačů, které nejsou organizací spravované (jako jsou například domácí počítače). Firmy ale nemohou předpokládat, že tyto externí počítače jsou bezpečné, ani nemohou spoléhat na to, že koncoví uživatelé nezanechají stopy po svém „chování" nebo činnosti. Realita je taková, že použití webového e-mailu, jako je například aplikace Microsoft Outlook Web Access, vede ke zvýšenému ohrožení podnikových informací...

A právě před tímto rizikem by organizace měla chránit zmiňovaná aplikace Symantec On-Demand Protection. Ta brání uživatele před možným únikem dat, blokuje škodlivý kód a současně umožňuje bezpečný přístup k podnikovému e-mailu kdykoli a odkudkoli. Virtuální pracovní plocha vytvořená aplikací pomáhá zabránit úniku důvěrných dat z nespravovaných počítačů tím, že vytváří bezpečné prostředí, které šifruje data a po skončení relace odstraňuje soubory. Tím se snižuje riziko úniku informací neúmyslným zanecháním dat v souborech mezipaměti a dočasných souborech.

Kontrola integrity hostitele navíc zaručuje, že nespravované koncové body, které se pokoušejí připojit k podnikovým sítím, mají přiměřenou ochranu a nainstalovaný bezpečnostní software. Aplikace navíc obsahuje i modul detekce škodlivého kódu na základě „chování", který blokuje hrozby jako programy zaznamenávající stisky kláves a programy pro zachycení údajů na obrazovce.

Další novinkou je aplikace Symantec On-Demand Protection for Web Applications 3.0, která nabízí v rámci podniku podobnou ochranu pro webové podnikové aplikace, jako jsou sítě SSL VPN, nebo podnikové webové portály intranetů a extranetů.

SYMANTEC: **On-demand protection.**

NOVINKA OD SPOLEČNOSTI TREND MICRO

Nejen proti spamu...

Společnost Trend Micro Incorporated ohlásila vylepšení produktu Trend Micro InterScan Gateway Security Appliance, který je určen pro správu zabezpečení obsahu ve středně velkých organizacích. Nově je tento produkt rozšířen i o technologii InterScan Gateway Security pro zjišťování důvěryhodnosti webových stránek, která je kompatibilní s technologií Total Web Threat Protection. Mezi další nové funkce patří ochrana proti obrázkovému spamu a prevence úniku dat. Za svou expertní antispamovou technologii nástroj nedávno získal certifikát prvotřídní kvality od společnosti West Coast Labs. V nedávném benchmarkovém testu nezávislé testovací agentury Opus One dosáhl navíc vícevrstvý antispam od společnosti Trend Micro nejvyššího skóre při zachytávání spamu (97,36 procenta) a srovnatelně nízké míry falešných pozitiv v porovnání s několika dalšími rozšířenými antispamovými řešeními.

YOUTUBE

Videa jako pašeráci virů

Jak oznamuje antivirová firma Panda Software, nový červ dokáže propašovat do počítače škodlivý kód prostřednictvím videí z YouTube. Záškodník pojmenovaný Spread-Banker.A změní položky v systémovém registru oběti tak, že poté nelze spustit Správce úloh, deaktivuje různé volby v menu Start a zablokuje přístup k webovým stránkám bezpečnostních firem. Škůdce kromě toho slouží svému programátorovi jako zloděj dat tak, že protokoluje uživatelem zadávaná hesla pro on-line transakce určitých bank, například Citibank, a přístupové údaje k internetovým hrám.

Červ nakazí počítač ve dvou stupních: v prvním kroku se zavede do počítače, což nejčastěji proběhne při využití sítí P2P, když uživatelé stahují soubor s názvem „sexogratis" nebo „crackwindowsvista". V druhém kroku se pak chybějící moduly červa dostanou do PC prostřednictvím zmanipulovaného videa z YouTube. Až do doby redakční uzávěrky rozpoznávaly červa jen proaktivní skenery. Na aktualizaci virových řetězců už se ale u všech velkých antivirových výrobců pracuje.

Info: www.pandasecurity.com

STUDIE SPOLEČNOSTI MCAFEE

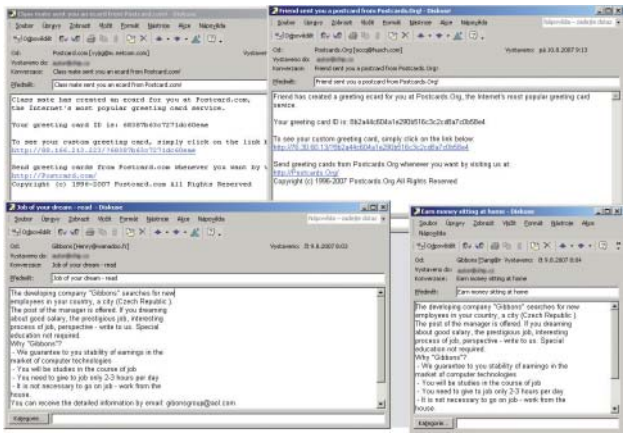
Hrátky s myslí

Společnost McAfee oznámila výsledky nového výzkumu, který mapuje, jak organizovaný zločin využívá psychologické triky k oklamání uživatelů PC. Výsledkem triků je obvykle důvěřivé předání osobních informací nebo přímý finanční zisk podvodníků. Na studii, jejímž cílem bylo porozumět trendům kybernetické kriminality, spolupracoval se společností McAfee přední soudní psycholog Clive Holin, profesor univerzity v britském Leicesteru.

Závěrem studie je zjištění, že zločinci zneužívají v poslední době v podvodných e-mailech stále častěji naše citlivá místa, kde jsme z psychologického pohledu nejvíce zranitelní. Používají stále dokonalejší techniky, jako je předpokládaná cena skutečné identity, dokáží předstírat přátelské žertování a pracují s lidskými emocemi, jako je strach, pocit nebezpečí a hrabivost. Jeden z příkladů zahrnutých do studie společnosti McAfee ukazuje, že dokonce i prostá zvědavost může mít neblahé následky a přinést podvodníkovi úspěch. Například jistá on-line reklama slibovala každému, kdo na ni klikne, infikovat počítač virem. Kliklo více než 400 lidí...

Podvodné taktiky

Studie ukazuje, jaké klíčové prvky obsahuje typický podvodný e-mail a k jakým aktivitám se snaží uživatele přesvědčit. Typické jsou například věty Click here for a reward (Klikněte sem a získejte odměnu) nebo Click here to avoid something you don't want to happen (Klikněte sem a vyhněte se něčemu, co nechcete, aby nastalo). Studie (v rozporu s oblíbeným názorem) ukazuje na nesprávnost představy, podle které se obětí internetových podvodů stávají pouze nezkušení uživatelé. Kybernetičtí zločinci jsou naopak úspěšní ve vztahu ke všem skupinám uživatelů. Profesor Clive Hollin uvedl: „Přesvědčivost komunikace je dána kombinací situačních a osobních faktorů. Většina lidí je ve vztahu k zavádějícím informacím zranitelná. Platí to bez ohledu na míru počítačových zkušeností uživatelů. Ačkoliv se úspěch řady podvodů dá vysvětlit naivitou, zavádějícími informacemi se nechávají oklamat i zkušení uživatelé."



HROZBY: Zábava, přátelé, peníze – lákadla se příliš nemění...

Hrozby se stále vyvíjejí

Studie Mind Games (Hrátky s myslí) společnosti McAfee ukazuje, že internetoví podvodníci zkoumají slabá místa potenciálních obětí a na tomto základě upravují své aktivity. Někteří uživatelé například sledují zpravodajské titulky podle emotivních výrazů nebo slov vyjadřujících obavy, jiní se zaměřují na velké sportovní události. Pomocí podobných poznatků pak mohou hry rozehrané internetovými zločinci působit jako autentické. Kybernetičtí útočníci se také „přiživují" na nových společenských trendech. Uživatelé aplikací, jako je MySpace či Facebook, jsou zvyklí na neformální e-maily i aktualizace webu. Často nedovedou posoudit legitimnost e-mailů nebo hypertextových odkazů a ve své důvěřivosti se stávají obětí jak phishingu, tak i podvodů souvisejících s krádeží identity. Podvodníci mají své aktivity často dobře promyšlené. Úspěšně začínají používat také způsoby manipulace, které zatím nejsou uživatelům příliš podezřelé, jako je například komunikace přes mobilní telefony.

F-SECURE

Antivirový nástroj vstupní branou hackerů

Společnost F-Secure oznámila dvě bezpečnostní mezery ve svých antivirových produktech. Útočníci tak mohou prostřednictvím zmanipulovaných souborů propašovat do počítače škodlivý kód a ochromit jím jeho činnost. Záplata už je k dispozici.

První mezera umožňuje využití přetečení bufferu při dekomprimaci archivů LHA. Útočník tak může způsobit zhroucení počítače. Druhá mezera se projevuje při zpracování tzv. I/O Request Packets (IRP) skenerem pracujícím v reálném čase. Lokální uživatelé tak mohou obdržet oprávnění správce a spouštět libovolné programy nebo také měnit bezpečnostní nastavení Windows. F-Secure však už distribuuje aktualizace. Ty se nainstalují automaticky prostřednictvím aktualizační funkce softwaru.

Info: www.f-secure.com

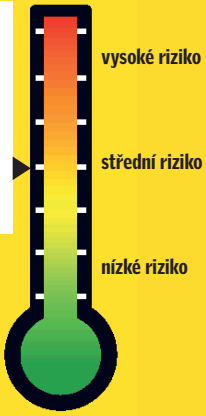
FIREFOX

Kritické chyby

V prohlížeči Firefox (verze nižší než 2.0.0.5) bylo objeveno několik důležitých chyb. Zranitelnosti mají velmi široký dopad, od obejití bezpečnostních nastavení, odkryti citlivých informací a útoku typu Denial of Service až po kompletní kompromitaci systému. Tři z těchto chyb byly identifikovány jako kritické. První zranitelnost se týká chyb v javascriptovém enginu, které umožní útočníkovi „shodit aplikaci" a případně spustit libovolný kód na cílovém stroji. Druhá kritická zranitelnost je způsobena některými vnějšími elementy dokumentu, které dovolí útočníkovi vyvolat event handler a spustit libovolný příkaz s vyššími systémovými právy. Třetí zranitelnost je způsobena spouštěním Firefoxu z prostředí MS Internet Explorer, které umožní spustit libovolný kód na cílovém stroji. Čtvrtá zranitelnost je způsobena problémy s „XPCNativeWrapper". V pátém případě se jedná o chybu neautorizovaného přístupu ke cachovaným dokumentům do „wyciwig://". Šestá chyba spočívá v odlišné interpretaci URL, Firefox v tomto případě interpretuje URL odlišně od operačního systému. Sedmá chyba spočívá v otevření podvrženého framu během načítání stránky. A konečně osmá zranitelnost je typu Cross-Site Scripting provedeného pomocí „addEventListener" a „setTimeout". Podrobnější informace najdete na adrese **www.mozilla.org/security/**. Opravená verze Firefoxu, poštovního klienta Thunderbird a prohlížeče Seamonkey jsou k dispozici na webu výrobce. Vzhledem k závažným chybám se doporučuje urychlený upgrade na verzi 2.0.0.6.

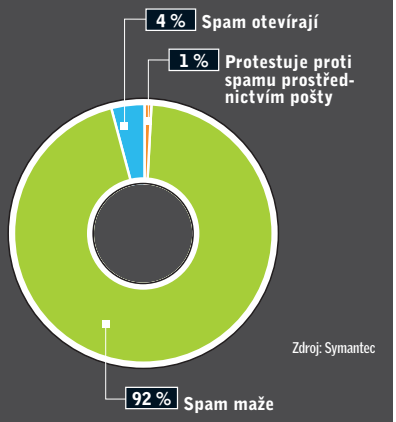
Barometr nebezpečí

Největší světový spammer je konečně za mřížemi. Přesto ještě existuje více než 200 spamových skupin, které rozesílají phishingové maily.



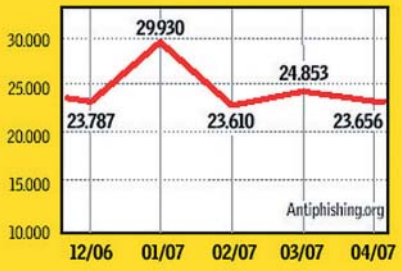
Chip vyhodnocuje potenciál webového nebezpečí na základě aktuálních bezpečnostních statistik.

Reakce na spam



Většina uživatelů reaguje správně a reklamní balast rovnou odstraňuje; všechno ostatní situaci jen zhoršuje.

Trendy phishingu



Méně phishingu: Důvodem je zlepšený ochranný software výrobců antivirů.

ČÍSLO MĚSÍCE

700 eur

se na webu platí za „MPack", nástroj, který skrze bezpečnostní mezery propašuje do počítače škodlivé programy.

APPLE MAC OS X

Sledovaná hrozba

Laboratoře McAfee (McAfee Avert Labs) monitorují vývoj nového škodlivého softwaru, cíleného proti operačnímu systému Apple Mac OS X. Jeho vývoj byl poprvé ohlášen koncem července na jednom blogu, oznámení však poté zmizelo. Nicméně kód dokazující proveditelnost (Proof-of-concept) exploitu na Macintoshi byl přidán do databáze hrozeb SecurityFocus. Ve zmíněném, již smazaném blogu předpokládaný tvůrce malwaru mj. naznačuje, že za svou práci dostal zaplaceno.

Výzkumník z laboratoří McAfee Avert Labs Francois Paget na jiném blogu uvažuje o těchto událostech: *„Tento příběh dokazuje dvě věci. Za prvé to, že se Macintosh díky procesoru od Intelu stal zajímavým cílem. Vize masového rozšíření škodlivého kódu je na Macintoshích reálnější než kdy jindy. A za druhé, že vábení peněz k tvorbě škodlivého kódu motivuje mnohé, třebas i zásadové lidi. Což je další důvod k obavám."*

Info: www.avertlabs.com/research/blog/index.php

MOZILLA FIREFOX

Phishingové mezery v přídavných modulech

Mnohá rozšíření Firefoxu se integrují bez bezpečnostního dotazu u aktualizačních serverů. Výsledkem je, že útočníci mohou v napadeném počítači spouštět škodlivé programy. V normálním případě se rozšíření Firefoxu uživatele dotáže ještě dříve, než se software dostane do počítače, v řadě případů je však toto hlášení vypnuto. Student Christopher Soghoian na svém blogu popisuje možnost, jak lze prostřednictvím útoku „man in the middle" přesvědčit oběť, že má co dělat s legitimním aktualizačním serverem. Je tomu tak například s nástrojovými lištami v Googlu, Yahoo, Ask a AOL. Pomocí může jedině odstranění těch rozšíření prohlížeče, která nezavádějí updaty prostřednictvím https.

Info: www.mozilla-europe.org

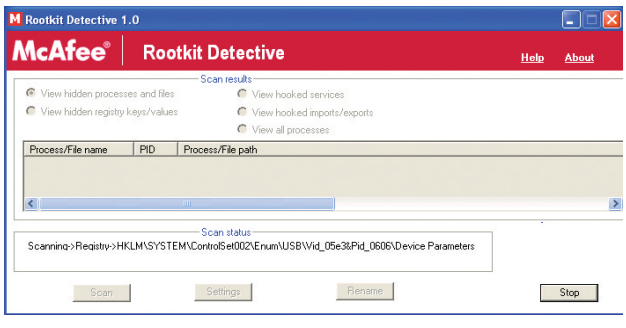
SOFTWARE MCAFEE

Rootkit Detective zdarma

Společnost McAfee nabízí nový a zdarma dostupný nástroj, který pomáhá uživatelům vyčistit počítače od nebezpečného kódu typu rootkit. Nástroj Rootkit Detective vyvinuly laboratoře Avert Labs. Kybernetičtí zločinci používají rootkity k tomu, aby na infikovaném počítači skryli další škodlivé programy. V loňském roce bylo zaznamenáno celkem 3284 rootkitů a jen za první polovinu letošního roku se toto číslo zvýšilo více než dvojnásobně, na 7325. První verze nástroje Rootkit Detective byla uvedena letos v lednu a již se dočkala více než 110 000 stažení.

Se škodlivými rootkity se na internetu nelegálně obchoduje. Někteří hackeři dokonce vytvářejí tyto nástroje za úplatu na objednávku. Tento typ softwaru se často používá ke skrytí zadních vrátek (backdoor), která narušiteli umožňují nepozorovaný přístup k počítači. Rootkity se obvykle šíří jako součást škodlivých programů typu trojský kůň nebo spolu se stažením nebezpečných dat. Někteří výrobci adwaru používají rootkity také ke skrytí svého softwaru.

Rootkit Detective je výkonný nástroj, který uživatelům umožňuje nahlédnout pod povrch operačního systému. Lze jej použít například ve chvíli, kdy dojde k náhlému zpomalení odezvy systému nebo k podezřelé síťové aktivitě. Nástroj Rootkit Detective zviditelňuje skryté procesy, položky registru i soubory a umožňuje je uživateli bezpečně odebrat nebo zakázat pomocí restartu systému. Tento nástroj navíc uživateli umožňuje zkontrolovat integritu paměti jádra (kernelu) systému počítače a zobrazit veškeré změny, které mohly také přispět k jeho ohrožení. Pomocí nástroje Rootkit Detective mohou koncoví uživatelé i firmy rovněž zasílat vzorky identifikovaných kódů laboratořím Avert Labs. Po provedení analýz bude vytvořena definice příslušného rootkitu a přidána ke klientských bezpečnostním produktům společnosti McAfee, což umožní vylepšit detekci rootkitů a možnosti zabezpečení obecně.



SUN

Trhliny v kancelářských balících

Dvě bezpečnostní mezery v OpenOffice a StarOffice mohou způsobit, že útočník spustí na PC cizí kód, aniž by to uživatel zpozoroval. První „netěsnost" se projevuje při zpracování dokumentů formátu RTF. Zmanipulované soubory pak způsobí přetečení bufferu – a útočník může nahrát škodlivý kód.

Druhou mezeru odhalili bezpečnostní experti při zpracování písem TTF. Preparovaný TTF soubor způsobí chybu v knihovně FreeType kancelářských balíků. Aplikace využívající tuto knihovnu pak havarují a spustí hackerův kód. Pro obě mezery jsou na stránce výrobce k dispozici aktualizace.

Info: www.sun.com

ZRANITELNÉ PROGRAMY

Nová bezpečnostní rizika

YAHOO MESSENGER

Děravé moduly

Kvůli chybě v ActiveX modulech Yahoo Messengeru mohou útočníci spouštět v napadeném počítači škodlivý kód, aniž by k tomu potřebovali oprávnění správce. ActiveX moduly slouží k podpoře webových kamer. Řešením je instalace nejnovější verze messengeru z webové stránky výrobce.

Info: www.yahoo.com

NOD32

Mezera v antiviru

Bezpečnostní mezera, která se objevuje v antivirovém nástroji NOD32 při zpracování názvů cest, umožňuje útočníkům převzít kontrolu nad počítačem. Hackerovi k tomu stačí založit v počítači soubor s nadměrně dlouhým názvem. Na stránkách výrobce už ale najdete záplatu...

Info: www.eset.com

KASPERSKY ANTIVIRUS

Nástroj proti virům s chybou

Existuje exploit, který způsobí havárii počítače chráněného antivirovým nástrojem. Útočník k tomu nepotřebuje ani oprávnění správce. Postiženy jsou verze 6 a 7 nástroje Kaspersky Antivirus.

Na webu výrobce je již k dispozici opravný patch, který tuto zranitelnost řeší. Po instalaci opravy je nutné restartovat počítač...

Info: www.kaspersky.com

WINDOWS

Pozor na aktualizace Windows

Trojské koně zneužívají aktualizační službu Windows ke stahování vlastních záškodnických rutin. Tímto způsobem se vyhnou rozpoznání softwarovými firewally. Microsoftu je problém znám, záplata však dosud není k dispozici. Integrita aktualizací Windows ohrožena není. Oprava by se měla objevit jednom z příštích balíků záplat...

Info: www.microsoft.com